摘　要

基于验证-工作双链的电子医疗记录管理系统

区块链技术因为其去中心化、不可篡改、可追溯、公开透明等特性，已经成为中心化问题的主流解决方案，除了最广为人知的加密货币领域以外，区块链在供应链和身份认证等领域也有广泛应用，得到了许多国家和机构的高度关注。但在实际应用中，小规模的区块链并不足够安全可靠，由于区块链共识机制的属性，如果对区块链发动 51%攻击将直接令其无法正常工作，虽然 51%攻击因为过高的攻击开销在大规模区块链中几乎不可能实现，但在小规模区块链中 51%攻击的攻击开销则往往在攻击者可接受的范围内，除了线上的 51%攻击，攻击者也可以线下贿赂节点管理员达到与 51%攻击同等效果的攻击，当攻击者从该次攻击中获取的利润明显高于此次攻击开销时，该区块链系统就存在极高的安全风险。为了解决此问题，本文提出了验证-工作双链架构作为解决方案，工作链是原系统中负责业务的小规模区块链，验证链是大规模的公链，为系统提供信任根，工作链节点定期将工作链区块的验证信息上传到验证链，当工作链受到攻击或产生争议时，正常节点可按照验证链上的验证信息根据受攻击程度恢复工作链或硬分叉工作链。

在医疗领域，电子医疗记录系统(EMR)与患者的生命健康息息相关，EMR 如果发生停机、数据被篡改等事故会导致难以估量的损失，除此以外，许多攻击者也将高价值的患者医疗隐私信息设为目标，伺机通过泄露医疗信息获取高额利润，所以 EMR 需要极高的安全性。为了解决 EMR 中心化导致的数据溯源、审计等环节低可信度的问题，许多研究者开始将区块链技术与 EMR 相结合，但目前所有研究者的研究都是基于单区块链的 EMR 系统，普遍忽略了上述单链规模较小时 EMR 的安全风险，因此本文选择在 EMR 领域完成验证-工作双链的实现，工作链负责 EMR 业务相关内容，类似单链 EMR 系统中的区块链，与 EMR 的最终用户打交道。验证链负责验证工作链区块，工作链的节点除了执行正常的工作链维护以外，他们还

会将自己的区块哈希值上传到验证链中，实现当工作链的数据被篡改时，节点们可以根据需要恢复工作链或硬分叉。

本文的主要工作如下：

1.设计并分析了验证-工作双链架构。为了避免与其他研究中意义不同的“双链”术语混淆，本文对验证-工作双链做出了标准化定义；为了解决攻击检测问题，本文设计了定期自检的被动验证流程和满足节点需求的主动验证流程；为了减少工作链受攻击后的影响，本文也设计了受攻击状态下工作链正常节点的硬分叉策略及其可行性，分析了工作链可能受到的单链攻击影响和双链系统可以解决单链问题的原因，证明了解决上述区块链安全问题的可行性。

2.设计并实现了基于验证-工作双链的 EMR 系统。本文对 EMR 软件的需求进行了分析，设计了 EMR 的整体架构，该系统的 EMR 业务包含身份注册、患者管理等功能，可以满足常见的 EMR 场景需求，为了贴合现实场景，本文设计的 EMR 数据类型模拟了各类医疗数据，并利用 IPFS 链下存储技术减轻区块链压力、增加去中心化程度；本文说明了区块链在 EMR 各层架构中的功能和作用；除此以外本文也对区块链技术选型进行了说明，分析了各类区块链存在的优劣势，选择使用以太坊 2.0 及其相关技术开发基于验证-工作双链的 EMR 系统；为了最大化该系统的去中心化程度，除了使用区块链技术以外，本文也使用了 IPFS 链下存储技术。

3. 通过实验，验证了基于验证-工作双链的 EMR 系统在效率、安全性方面的进步性。本文对基于双链的 EMR 系统业务效率、工作链功能和受攻击场景都进行了测试实验，为了与对应基于单链的 EMR 表现进行对比，并消除访问、传输等事件对测试结果的影响，本文实现了一个具有与双链架构相同 EMR 模块和工作链的基于单链的 EMR 系统，对其进行相同的测试。实验结果表明，在测试环境下，基于双链架构的 EMR 相比基于单链架构的 EMR 额外性能损耗在 10ms 以内，但双链架构正常节点可以用 0.8s 探测到 51%攻击行为，并进行区块链恢复或硬分叉，这是单链架构无法做到的，本文也对导致评测结果可能的原因做出了分析和推断。

通过以上工作，本文说明了基于验证-工作双链的 EMR 系统相比于基于单链

的 EMR 系统具有更优秀的安全性，面对低中心化性质攻击时可以有效恢复工作链，面对高中心化性质攻击可以根据节点需求提供硬分叉参考，双链带来的效率损耗几乎可以忽略不计。

关键词：

区块链，EMR，双链，以太坊

Abstract

Electronic medical record management system based on verification-working double blockchain

As Blockchain technology has become a mainstream solution to the centralization problem because of its characteristics of decentralization, non-tampering, traceability, openness and transparency. In addition to the most well-known cryptocurrency field, blockchain is also widely used in fields such as supply chain and identity authentication, and has received great attention from many countries and institutions. However, in practical applications, small-scale blockchains are not safe and reliable enough. Due to the nature of the blockchain consensus mechanism, if a 51% attack is launched on the blockchain, it will directly make it unable to work normally.

Although a 51% attack is almost impossible in a large-scale blockchain due to the high attack overhead, the attack overhead of a 51% attack in a small-scale blockchain is often within the acceptable range of the attacker. In addition to the online 51% attack, the attacker can also bribe the node administrator offline to achieve the same effect as the 51% attack. When the profit obtained by the attacker from the attack is significantly higher than the attack cost, the blockchain system has extremely high security risks. In order to solve this problem, this paper proposes a verification-work dual-chain architecture as a solution. The working chain is a small-scale blockchain responsible for business in the original system, and the verification chain is a large-scale public chain that provides a root of trust for the system. Working-chain nodes regularly upload the

verification information of working chain blocks to the verification chain. When the working chain is attacked or disputes arise, normal nodes can restore the working chain or hard fork the working chain according to the degree of attack according to the verification information on the verification chain.

In the medical field, the electronic medical record system (EMR) is closely related to the life and health of patients. If the EMR has accidents such as downtime and data tampering, it will cause inestimable losses. In addition, many attackers also target high-value private medical information of patients, waiting for an opportunity to obtain high profits by leaking medical information, so EMR requires extremely high security. In order to solve the problems of low credibility such as data traceability and auditing caused by the centralization of EMR, many researchers have begun to combine blockchain technology with EMR, but currently all researchers' research is based on a single blockchain EMR system , ignoring the security risk of EMR when the scale of the single chain is small, so this article chooses to complete the verification in the field of EMR - the realization of the work double chain, the working chain is responsible for the EMR business related content, similar to the blockchain in the single-chain EMR system, dealing with the end users of EMR. The verification chain is responsible for the verification of the working chain blocks. In addition to performing normal working chain maintenance, the nodes of the working chain will also upload their own block hash values to the verification chain, so that when the data of the working chain is tampered with, nodes can restore the working chain or hard fork as needed.

The main work of this paper is as follows:

1. Design and analyze the verification-working double-chain architecture. In order to avoid confusion with the "double-chain" term with different meanings in other studies, this paper makes a standardized definition of the verification-working double-chain; for attack detection in some scenarios, this paper designs a passive verification process for regular self-inspection and an active verification process to meet the needs of nodes; in order to reduce the impact of the working chain after being attacked, this paper also designs the hard fork strategy and its feasibility of the normal nodes of the working chain under attack , analyzed the possible impact of single-chain attacks on the working chain and the reason why the double-chain system can solve the single-chain problem.

2. Design and implement the EMR system based on the verification-working double chain. This paper analyzes the requirements of EMR software and designs the overall architecture of EMR. The EMR business of the system includes functions such as identity registration and patient management, which can meet the needs of common EMR scenarios. In order to fit the real scene, the EMR data type designed in this paper simulates various medical data, and uses IPFS off-chain storage technology to reduce the pressure on the blockchain and increase the degree of decentralization; This article explains the functions and functions of blockchain in the architecture of each layer of EMR; in addition, this article also explains the selection of blockchain technology, analyzes the advantages and disadvantages of various blockchains, In the end, I chose to use Ethereum 2.0 and related technologies to develop an EMR system based on the verification-work double chain; in order to maximize the degree of decentralization of the system, in addition to using blockchain technology, this paper also

uses IPFS off-chain storage technology.

3. Through experiments, the progress of the EMR system based on the verification-work double chain in terms of efficiency and security has been verified. This paper conducts test experiments on the business efficiency, working chain function and attack scenarios of the EMR system based on the double chain. This paper implements a single-chain-based EMR system with the same EMR module and working chain as the double-chain architecture, and performs the same tests on it. The experimental results show that in the test environment, the EMR based on the dual-chain architecture has an additional performance loss of less than 10ms compared to the EMR based on the single-chain architecture, but the normal nodes of the dual-chain architecture can detect 51% attacks in 0.8s and carry out blockchain recovery or hard fork, which is impossible for a single-chain architecture. This article also analyzes and infers the possible reasons for the evaluation results.

Through the above work, this paper shows that the EMR system based on the verification-work double chain has better security than the single-chain EMR system, and can effectively restore the working chain in the face of low-centralization attacks. In the face of highly centralized attacks, hard fork references can be provided according to node requirements, and the efficiency loss caused by the double chain is almost negligible.

Keywords:

blockchain, EMR, double blockchain, Ethereum

目　　录

第 1 章 引言

1.1 研究背景和意义

区块链技术作为中心化问题的主流解决方案之一备受关注，具有去中心化、可追溯、公开透明、不可篡改等特性，正因为这些特性，区块链技术在很多领域都有应用，除了火热的加密货币领域以外，在供应链、身份认证等诸多领域也扮演了重要的角色。

随着加密货币市场的指数级增长、区块链技术的热度也居高不下，许多科研机构、经济组织甚至政府开始加大对区块链领域的投入。例如欧盟把推动区块链技术的发展和应用作为长期战略，在 2022 年 10 月更是通过了里程碑式的《加密资产市场监管法案》[1]，旨在规范加密货币资产市场、支持区块链技术在金融领域的创新、激发区块链的竞争潜力。中国工信部早在 2016 年 10 月就发布了区块链领域的白皮书[2]，总结了我国区块链技术的发展历程，评估了当下区块链的研究趋势，预设了未来区块链可能的发展方向和创新角度。同年 12 月，国务院在“十三五”中第一次提出将“区块链”评价为战略性前沿技术[3]，并写入规划，标志着我国开始高度重视区块链技术，加大区块链领域扶持力度。2019 年国家互联网信息办公室制定了区块链服务的规范性管理政策，以此加强对区块链领域的监管[4]。在同年的十八大中，习近平主席重点强调区块链技术自主创新的重要性，为区块链技术的重要性做出定论。区块链技术同样写入了 2021 年的“十四五”规划中，并将作为中国的长期发展战略的重要组成部分[5]。

虽然从应用角度区块链的应用领域较为广泛，应用结合度也较为成熟，但在安全方面对于较小规模区块链的安全研究较为匮乏，这些从应用角度开展的研究也没有考虑使用较小规模区块链时安全隐患。因为区块链共识机制的属性，区块链在攻击者 51%攻击的情况下都无法保证区块链的正常运行，虽然在